REMARKS:

This paper is herewith filed in response to the Examiner's final Office Action mailed on July 6, 2007 for the above-captioned U.S. Patent Application. This office action is a rejection of claims 1-14 of the application.

More specifically, the Examiner has rejected claims 1-14 under 35 USC 102(e) as anticipated by Win et al. (US6,453,353). The applicant respectfully traverses the rejections.

The Applicant respectfully notes that Win et al. relates to controlling access to resources "after a user is authenticated," (col. 10, line 43).

Win et al. discloses:

> "After a user is authenticated, the Authentication Client module 414 calls the Authorization service of Access Server 106. In response, the Authorization service requests **profile information about the user** from the Registry Server 108, as shown by state 520. In state 522, Registry Server 108 returns the profile information to Access Server 106. **The profile information may comprise the user's name, locale information, IP address, and information defining roles held by the user. The Authorization service creates a "user cookie" 528 and "roles cookie" 530, which are used to convey profile information to browser 100**. The "user cookie" contains a subset of the user profile information. The "roles cookie" contains a list of the user's roles," (emphasis added), (col. 10, lines 43 to 55).

The Applicant respectfully asserts that the cookie in Win et al. which are created using "user profile information" and "a list of the user's roles" is seen as entirely distinguishable from the attribute certificate which is based in part on the **capabilities of the network device** as in the claimed invention. The Applicant contends that a cookie in Win et al. which comprises "the user's name, locale information, IP address, and information defining roles held by the user" is merely **identifying information** used to control access following authentication. The Applicant contends that the cookie in Win et al. can not be seen to disclose or suggest "**an attribute**

[certificate] based, in part, on a capability of the network device," as in claim 1.

In the Response to Arguments section of the Office Action the Examiner states:

> "Applicant argues that Win does not teach or suggest determining an attribute based, in part, on a capability of the network device. In response to applicant's argument, **the examiner submits that Win does teach or suggest the feature of determining an attribute based, in part, on a capability of the network device as shown in abstract, figure 1, col. 6, lines 58-65, col. 11, line 42-col. 12, line 8, col. 24, lines 24-55**," (emphasis added).

As cited Win et al. discloses:

> "When the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource. **The cookie is also used by the resource to return information that is customized based on the user's name and roles**," (emphasis added), (col. 6, lines 58-65).

The Applicants contend that this reference cited by the Examiner **supports** the Applicants contention that the cookie in Win et al. is simply based on user profile information.

Further, as cited by the Examiner Win et al. discloses:

> "FIG. 5E is a state diagram of a method delivering a role-specific access menu to a network user. In the preferred embodiment, after the Authorization service of Authentication Client module 414 has looked up a user's roles from the Registry Server 108, Access Menu Module 412 uses a Personalized Menu Service to build a list of resources 208 that are available to the user. As shown by state 538, **Access Server 106 determines that the user is authentic, using the steps described above, and requests Registry Server 108 to return a profile of the user**. In state 540, **Registry Server 108 returns profile information for the user to Access Server 106. In response, the Personalized Menu Service constructs a personalized menu of resources showing only those resources that the user is authorized to access according to the user's profile information, including the user's roles and privileges**. [and]

> Significantly, in this configuration, after the personalized menu is returned to the browser, no additional login is required to access additional resources in the personalized menu, until the user logs off, quits the browser 100, or until the expiration time of the cookies is reached," (emphasis added), (col. 11, line 42 to col. 12, line 8).

Here Win et al. merely discloses that a personalized menu is constructed using the "user's roles and privileges" received from the Registry Server 108. The personalized menu contains links to only those resources the user profile indicates the user is authorized to access. The Applicants contend that the Examiner has not shown here that Win et al. discloses an "attribute based, in part, on **a capability of the network device**," as in claim 1.

In addition, as cited Win et al. discloses:

> "Further, the system is based on an additive data model in which higher levels of user authorization are constructed by incrementally adding privileges and rights to roles that have restrictions on user action. **Roles specify which resources a user may access. Assigning a role to a user or deleting a role from a user can add or delete access to all resources with that role. Similarly, adding a role to a resource or removing a role from a resource can give or take away access to that resource from all users with that role.** The Administration Application allows administrators to make such changes with a single click, resulting in significant administration time savings," (emphasis added), (col. 24, lines 26-47).

Again the Applicants can find nothing in the reference cited which discloses "an attribute based, in part, on **a capability of the network device**," as in claim 1. The Applicants submit that the roles are related to assigned user functions. In Win et al. roles are created allowing or not allowing access to resources based on **user privileges** that may be set by an administrator. The Applicant contends that there is nothing in all of Win et al. which discloses "an attribute based, in part, on **a capability of the network device**," as in claim 1.

Win et al. discloses:

> "Defining roles involves identifying role names, identifying functional groups,

> and defining user types. It may also involve **associating roles to user types. Roles are developed by listing functions or capacities in which a person might act when they access Web resources and their functional group, department, or organizational unit.** Roles should accurately represent the actual work roles carried out by individuals in the organization and the current kinds and levels of access that are appropriate for the resources of the organization," (emphasis added), (col. 13, lines 54-59).

Clearly, allowing access to resources based on associated user roles as in Win et al does not relate to attribute certificates based in part on a capability of **a network device** as in claim 1.

The Applicants respectfully contend that the application of Win et al. in the rejection under 35 USC 102(e) is improper.

The Applicants note that a 35 USC 102 rejection requires that the cited art **disclose to the specificity of the rejected claim**; Verve, LLC v. Crane Cams, Inc., 311 F.3d 1116, 1120, 65 USPQ2d 1051 (Fed. Cir. 2002) ("**A single reference must describe the claimed invention with sufficient precision and detail to establish that the subject matter existed in the prior art**").

For at least the reasons stated the Applicants contend that Win et al. can not be seen to anticipate claim 1 and the rejection of claim 1 should be removed.

In addition, as the independent claims 9 and 14 recite a similar feature of claim 1, for at least the reasons stated above Win et al. does not anticipate these claims, and all the claims 1, 9, and 14 should be allowed.

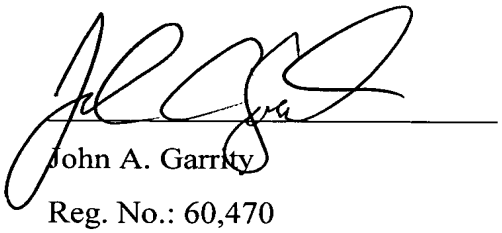
Furthermore, for at least the reason that the claims 2-8; and 10-13; depend from claims 1, and 9, respectively, Win et al. does not disclose or suggest these claims, and all the claims 1-14 should be allowed.

Based on the above explanations and arguments, it is clear that Win et al. cannot be seen to anticipate claims 1-14. The Examiner is respectfully requested to reconsider and remove the

rejections of claims 1-14 and to allow all of the pending claims 1-14 as presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' agent at the telephone number indicated below.

Respectfully submitted:



10/6/2007

John A. Garrity
Reg. No.: 60,470
Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: jgarrity@hspatent.com

Date

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450,

Alexandria, VA 22313-1450.

10/8/2007 Claire F. Muir

Date Name of Person Making Deposit